

PATENT ABSTRACTS OF JAPAN

(2)

(11)Publication number : 2003-228552

(43)Date of publication of application : 15.08.2003

(51)Int.Cl.

G06F 15/00

(21)Application number : 2002-304068

(71)Applicant : HEWLETT PACKARD CO <HP>

(22)Date of filing : 18.10.2002

(72)Inventor : TARQUINI RICHARD PAUL
SCHERTZ RICHARD LOUIS
GALES GEORGE SIMON

(30)Priority

Priority number : 2001 001728

Priority date : 31.10.2001

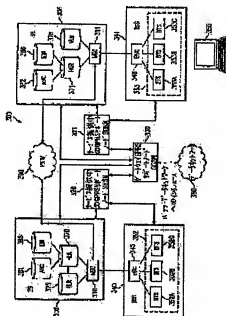
Priority country : US

(54) MOBILE DEVICE FOR MOBILE TELECOMMUNICATION NETWORK PROVIDING
INTRUSION DETECTION

(57)Abstract:

PROBLEM TO BE SOLVED: To provide a mobile device for a mobile telecommunications network providing intrusion detection.

SOLUTION: The mobile device (355) operable in a mobile telecommunications network (300) is equipped with a memory module (274) for storing data in machine readable format for retrieval and execution by a central processing unit (272) and an operating system (275) operable to execute an intrusion detection application (91) stored in the memory module (274).



(51) Int.Cl.⁷

G 0 6 F 15/00

識別記号

3 3 0

F I

G 0 6 F 15/00

テーマコード* (参考)

3 3 0 A 5 B 0 8 5

審査請求 未請求 請求項の数 1 O L (全 13 頁)

(21) 出願番号 特願2002-304068(P2002-304068)

(22) 出願日 平成14年10月18日 (2002.10.18)

(31) 優先権主張番号 1 0 / 0 0 1 , 7 2 8

(32) 優先日 平成13年10月31日 (2001.10.31)

(33) 優先権主張国 米国 (U S)

(71) 出願人 398038580

ヒューレット・パッカード・カンパニー
HEWLETT-PACKARD COMPANYアメリカ合衆国カリフォルニア州パロアルト
ハノーバー・ストリート 3000

(72) 発明者 リチャード・ポール・タークニ

アメリカ合衆国27502ノース・カロライナ
州アベックス、パーメイヤー・プレイス
110

(74) 代理人 100081721

弁理士 岡田 次生 (外 2 名)

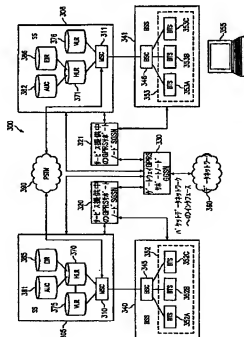
最終頁に続く

(54) 【発明の名称】 不正侵入検出を提供するモバイル通信ネットワークのためのモバイル機器

(57) 【要約】

【課題】 不正侵入検出を提供するモバイル通信ネットワークのためのモバイル機器を提供する。

【解決手段】 モバイル通信ネットワーク (300) において動作可能なモバイル機器 (355) であって、中央演算処理装置 (272) による検索および実行のためにマシン読み取り可能フォーマットでデータを格納するメモリモジュール (274) と、該メモリモジュール (274) に格納される不正侵入検出アプリケーション (91) を実行するように動作可能なオペレーティングシステム (275) と、を備える。



【特許請求の範囲】

【請求項1】 モバイル通信ネットワークにおいて動作可能なモバイル機器であって、中央演算処理装置による検索および実行のためにマシン読み取り可能フォーマットでデータを格納するメモリモジュールと、該メモリモジュールに格納される不正侵入検出アプリケーションを実行するように動作可能なオペレーティングシステムと、を備えるモバイル機器。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、ネットワーク技術に関し、特に、不正侵入検出を提供するモバイル通信ネットワークのためのノードおよびモバイル機器に関する。

【0002】関連出願の相互参照

本特許出願は、2001年10月31日付で出願され本願と共に譲渡された「METHOD AND COMPUTER READABLE MEDIUM FOR SUPPRESSING EXECUTION OF SIGNATURE FILE DIRECTIVES DURING A NETWORK EXPLOIT」と題する同時係属中の米国特許出願第10/003,501号、2001年10月31日付で出願され本願と共に譲渡された「SYSTEM AND METHOD OF DEFINING THE SECURITY CONDITION OF A COMPUTER SYSTEM」と題する米国特許出願第10/001,431号、2001年10月31日付で出願され本願と共に譲渡された「SYSTEM AND METHOD OF DEFINING THE SECURITY VULNERABILITIES OF A COMPUTER SYSTEM」と題する米国特許出願第10/001,410号、2001年10月31日付で出願され本願と共に譲渡された「SYSTEM AND METHOD OF DEFINING UNAUTHORIZED INTRUSION ON A COMPUTER SYSTEM」と題する米国特許出願第10/002,695号、2001年10月31日付で出願され本願と共に譲渡された「NETWORK INTRUSION DETECTION SYSTEM AND METHOD」と題する米国特許出願第10/002,423号、2001年10月31日付で出願され本願と共に譲渡された「NODE, METHOD AND COMPUTER READABLE MEDIUM FOR INSERTING AN INTRUSION PREVENTION SYSTEM INTO A NETWORK STACK」と題する米国特許出願第10/001,445号、2001年10月31日付で出願され本願と共に譲渡された「METHOD, COMPUTER-READABLE MEDIUM, AND NODE FOR DETECTING EXPLOITS BASED ON AN INBOUND SIGNATURE OF THE EXPLOIT AND AN OUTBOUND SIGNATURE IN RESPONSE THEREOF」と題する米国特許出願第10/003,815号、2001年10月31日付で出願され本願と共に譲渡された「NETWORK, METHOD AND COMPUTER READABLE MEDIUM FOR DISTRIBUTED SECURITY UPDATES TO SELECT NODES ON A NETWORK」と題する米国特許出願第10/001,446号、2001年10月31日付で出願され本願と共に譲渡された「METHOD, COMPUTER READABLE MEDIUM

AND NODE FOR A THREE-LAYERED INTRUSION PREVENTION SYSTEM FOR DETECTING NETWORK EXPLOITS」と題する米国特許出願第10/003,747号、2001年10月31日付で出願され本願と共に譲渡された「SYSTEM AND METHOD OF AN OS-INTEGRATED INTRUSION DETECTION AND ANTI-VIRUS SYSTEM」と題する米国特許出願第10/002,072号、2001年10月31日付で出願され本願と共に譲渡された「METHOD, NODE, AND COMPUTER READABLE MEDIUM FOR IDENTIFYING DATA IN A NETWORK EXPLOIT」と題する米国特許出願第10/002,697号、2001年10月31日付で出願され本願と共に譲渡された「NODE, METHOD AND COMPUTER READABLE MEDIUM FOR OPTIMIZING PERFORMANCE OF SIGNATURE RULE MATCHING IN A NETWORK」と題する米国特許出願第10/003,820号、2001年10月31日付で出願され本願と共に譲渡された「METHOD, NODE AND COMPUTER READABLE MEDIUM FOR PERFORMING MULTIPLE SIGNATURE MATCHING IN AN INTRUSION PREVENTION SYSTEM」と題する米国特許出願第10/003,819号、2001年10月31日付で出願され本願と共に譲渡された「USER INTERFACE FOR PRESENTING DATA FOR AN INTRUSION PROTECTION SYSTEM」と題する米国特許出願第10/002,694号、2001年10月31日付で出願され本願と共に譲渡された「METHOD AND COMPUTER-READABLE MEDIUM FOR INTEGRATING A DECODE ENGINE WITH AN INTRUSION DETECTION SYSTEM」と題する米国特許出願第10/003,510号、2001年10月31日付で出願され本願と共に譲渡された「SYSTEM AND METHOD OF GRAPHICALLY DISPLAYING DATA FOR AN INTRUSION PROTECTION SYSTEM」と題する米国特許出願第10/002,064号、および2001年10月31日付で出願され本願と共に譲渡された「SYSTEM AND METHOD OF GRAPHICALLY CORRELATING DATA FOR AN INTRUSION PROTECTION SYSTEM」と題する米国特許出願第10/001,350号に関連する。

【0003】

【従来の技術】サービス拒否(DoS)攻撃ユーティリティ等ネットワーク不正攻撃ツールはますます精巧になってきており、また技術の進展により実行が簡単になってきている。比較的単純な攻撃者は、1つまたは複数の標的とする設備に向けたコンピュータシステム毀損(compromises)をアレンジする。またはこれに関わることができ。ネットワークシステム攻撃(本明細書では不正侵入とも称する)は、コンピュータまたはコンピュータネットワークの不正または悪意を持った使用であり、1つまたは複数の選ばれた標的に対する連係攻撃において数百または数千ものプロセッサとされない、あるいは毀損されたインターネットノードが一線に関わる可能性がある。

【0004】クライアント/サーバモデルに基づくネッ

ネットワーク攻撃ツールは、標的としたネットワークまたは機器に対するネットワーク攻撃の実行に好ましいメカニズムになった。セキュリティに欠陥のあるネットワークにおける大容量シシは、分散攻撃の踏み台として攻撃者により望まれることが多い。大学のサーバは通常、高い接続性および大容量を有するが、比較的平凡なセキュリティを有することを特徴とする。このようなネットワークはまた、ネットワーク攻撃への関与に対してネットワークをさらに脆弱にする経験の浅いまたは仕事の負荷が重過ぎるネットワーク管理者を有することが多い。

【0005】ネットワーク媒体を介してのデータ伝送を拠り所とするサービス拒否ユーティリティ等悪意を持った攻撃アプリケーションを含むネットワーク攻撃ツールは、伝送データ中に特徴的な「シグネチャ (signature)」または認識可能なパターンを有することが多い。

シグネチャは、1つまたは複数のパケットに含まれる認識可能なシーケンスの特定のサブセットおよび/または認識可能なデータを含むもの。シグネチャ解析がネットワーク不正侵入防御システム (IPS) によって行われることが多く、これは、パターンマッチングアルゴリズムとして実施することができ、他のシグネチャ認識能力ならびにより高いレベルのアプリケーション監視ユーティリティを含むことができる。単純なシグネチャ解析アルゴリズムは、悪意のあるアプリケーションに関連するものと識別されている特定のストリングを探索することができる。ストリングがネットワークデータストリーム内で識別されると、そのストリングを搬送する1つまたは複数のパケットを「悪意のある」または攻撃性のあるものと識別することができ、次いでIPSが、フレームの識別の記録、対策の実行、または別のデータ保存または保護対策の実行等、複数のアクションの任意の1つまたは複数を実行することができる。

【0006】不正侵入防御システム (IPS) は、コンピュータシステムまたはコンピュータシステムネットワークに対する攻撃の識別を試みる技術を含む。多くの種類のIPSが存在し、それぞれは概してネットワークベース、ホストベース、あるいはノードベースのIPSのいずれかに分類される。

【0007】ネットワークベースのIPS機器は通常、データパケットを検査して既知の攻撃シグネチャと一致するかどうかを判定するために、ネットワーク上の戦略的な場所に配置される専用システムである。パケットを既知の攻撃シグネチャと比較するため、ネットワークベースのIPS機器は、受動的なプロトコル解析と呼ばれるメカニズムを利用して、ネットワーク上のすべてのトラフィックを目立たないように監視、すなわち「スニッピング (sniff)」し、未処理のネットワークトラフィックから見分けることのできる低レベルのイベントを検出する。ネットワーク攻撃はパターンまたは、ネットワークフレームの他の観察可能な特徴を識別することによ

て検出することでもできる。ネットワークベースのIPS機器は、ネットワークフレームおよびパケットをパースし、ネットワークで使用されるプロトコルに基づいて個々のパケットを解析することによってデータパケットのコンテンツを検査する。ネットワークベースのIPS機器は、ネットワークトラフィックを目立たないように監視する。すなわち、他のネットワークノードは、ネットワークベースのIPS機器の存在に気付かなくてもよく、多くの場合は気付かない。受動的な監視は通常、ネットワークインタフェース機器の「プロミスキスマード」アクセスの実施によりネットワークベースのIPS機器によって実行される。プロミスキスマードで動作中のネットワークインタフェース機器は、パケットがアドレス指定された宛先ノードに関係なく、同軸ケーブル、100BASE-T、または他の伝送媒体等ネットワーク媒体から直接パケットを複製する。したがって、ネットワークベースのIPS機器がデータを検査することなくネットワーク伝送媒体を介してデータを伝送する単純な方法はないため、ネットワークベースのIPS機器は、IPS機器が嗅ぎ取るすべてのネットワークトラフィックを取り込み解析する。疑いのあるパケット、すなわちネットワークベースのIPS機器により発生を監視される既知の攻撃シグネチャに対応する属性を有するパケットが識別されると、これによって警告を生成し、ネットワークの専門家がセキュリティ対策を講じることができるよう、IPSの管理モジュールに伝送することができ。ネットワークベースのIPS機器は、リアルタイムで動作するというさらなる利点を有するため、発生時に攻撃を検出することが可能である。さらに、ネットワークベースのIPS機器は、単一ネットワークパケットである「最小単位 (atomically)」で識別することのできない、疑いがあると識別された攻撃パケットの蓄積および格納が必要な状態ベースのIPSセキュリティ対策の実施に理想的なものである。たとえば、伝送制御プロトコル (TCP) 同期 (SYN) フラッド攻撃は、単一のTCP SYNパケットで識別することは不可能であり、観して定義された時間期間にわたり予め定義された閾値を超えるTCP SYNパケットのカウンタを蓄積することによって識別される。したがって、ネットワークベースのIPS機器は、ローカルネットワーク媒体を渡るこのようなTCP SYNパケットをすべて検出し、よってかかるイベントを適宜保存しその頻度を解析することができるため、状態ベースのシグネチャ検出の実施に理想的なプラットフォームである。

【0008】しかし、ネットワークベースのIPS機器はしばしば、大量の「誤検知」、すなわち誤った攻撃診断を発生する。ネットワークベースのIPS機器による誤検知診断は、部分的に、暗号化され、任意の数のネットワークがサポートするプロトコルフォーマットされるIPSによって取り込まれるすべてのネットワーク

トラフィックの受動的な解析中に生じるエラーに起因する。ネットワークベースのIPSによるコンテンツスキャンは、暗号化されたリンクに対しては不可能であるが、プロトコルヘッダに基づくシグネチャ解析は、リンクが暗号化されているか否かに関わらず実行することができる。加えて、ネットワークベースのIPS機器は、高速ネットワークでは効果的ではないことが多い。高速ネットワークがより一般的になるため、リンク上のすべてのパケットのスニффリングを試みるソフトウェアベースネットワークベースのIPS機器の信頼性は低くなる。最も重要なことに、ネットワークベースのIPS機器は、ファイアウォール保護システムと一体化し、これと共に動作しなければ、攻撃を阻止することができない。

【0009】ホストベースのIPSは、アプリケーションレイヤデータを監視することによって不正侵入を検出する。ホストベースのIPSは、インテリジェントエージェントを採用して、疑いのあるアクティビティについてコンピュータ監査ログを連続して調べ、ログにおける各変化を攻撃シグネチャまたはユーザプロファイルのライブラリと比較する。ホストベースのIPSはまた、予期せぬ変化について主要なシステムファイルおよび実行可能ファイルをポーリングすることもできる。ホストベースのIPSは、IPSユーティリティが保護するよう割り当てられたシステム上に常駐することからそう呼ばれる。ホストベースのIPSは通常、各種アプリケーションが維持するアプリケーションログを検査するアプリケーションレベルの監視技法を採用する。たとえば、ホストベースのIPSは、失敗したアクセス試行および/またはシステム構成への変更を記録するデータベースエンジンを監視する。疑いがあると識別されたデータベースログから読み出されるイベントが識別されると、警告を管理ノードに提供することができる。ホストベースのIPSでの誤検知は、概して非常に少ない。しかし、log-watcher等ホストベースのIPSは概して、すでに行われた不正侵入の識別に限定され、かつ単一ホストに発生したイベントに限定される。log-watcherはアプリケーションログの監視に頼るため、記録された攻撃に起因するあらゆるダメージは概して、IPSにより攻撃が識別されるときには発生してしまっている。ホストベースのIPSによっては、「フッキング(hooking)」または「傍受」オペレーティングシステムアプリケーションログラングインタフェース等不正侵入防御機能を実行して、不正侵入に関連すると見られるアプリケーションレイヤアクティビティに基づく、IPSによる防御動作の実行を促進するものもある。このようにして検出される不正侵入はすでに任意のより低いレベルのIPSにバイパスされているため、ホストベースのIPSは、ネットワーク攻撃に対抗する防護の最後の砦を表す。しかし、ホストベースのシステム

は、プロトコルイベント等低レベルのネットワークイベントの検出にはほとんど役に立たない。

【0010】ノードベースのIPSは、不正侵入検出および/または保護技術を保護中のシステムに適用する。ノードベースのIPS技術の例は、インライン不正侵入検出である。ノードベースのIPSは、保護したいネットワークの各ノードにおいて実施することができる。インラインIPSは、保護されたネットワークノードのプロトコルスタックに組み込まれる不正侵入検出技術を含む。インラインIPSは、ネットワークベースのソリューションに固有の欠点の多くを克服する。上述したように、ネットワークベースのソリューションは概して、所与のリンク上のネットワークトラフィックすべてを監視しようとするため、高速ネットワークを監視する場合には効果的ではない。しかし、インライン不正侵入防御システムは、インラインIPSがインストールされたノードに向けられたトラフィックしか監視しない。したがって、攻撃パケットは、標的とする機器のプロトコルスタックを通過しなければならないため、標的とするマシン上のインラインIPSを物理的に迂回することができない。攻撃パケットによるインラインIPSのある迂回は、全体的にIPSを「論理的に」迂回することによって行われなければならない、すなわち、インラインIPSを避ける攻撃パケットは、インラインIPSがその攻撃パケットを識別することができないか、または不適切に識別することになるようにしなければならない。加えて、インラインIPSは、ネットワークIPSと同様にホストノードには低レベルの監視および検出能力を提供し、プロトコル解析およびシグネチャマッチング、または他のホストトラフィックの低レベルの監視またはフィルタリングを提供することができる。インラインIPS技術によって提供される最も重要な利点は、攻撃が発生する際に検出されることである。ホストベースのIPSは、システムログの監視により攻撃を判断するが、インライン不正侵入検出は、ネットワークトラフィックの監視およびホストサーバに対する攻撃の一部であると判断されたパケットの分離を含むため、インラインIPSが攻撃の進行を実際に防御することが可能である。パケットが攻撃の一部であると判断される場合、インラインIPSレイヤはそのパケットを破棄し、よってそのパケットが、攻撃パケットによってダメージが生じるプロトコルスタックの上位レイヤに到達しないようにし、その効果は、インラインIPSをホストするサーバのローカルファイアウォールを本質的に創り出し、インターネット等外部ネットワークあるいはネットワーク内からの脅威からサーバを保護することである。さらに、インラインIPSレイヤは、インラインIPSが暗号化リンクを使

用するネットワーク上で効果的に動作するように、パケットが暗号化されていないレイヤにおけるプロトコルスタック内に組み込むことができる。加えて、インラインIPSは、インラインIPSをホストするサーバに向けられたインバウンドトラフィックおよびそのサーバから発せられるアウトバウンドトラフィックそれぞれがプロトコルスタックを通過しなければならないため、出て行くトラフィックを監視することが可能である。

【0011】インラインIPS技術の利点は数多いが、かかるシステムの実施には欠点がある。インライン不正侵入検出は概して、プロセス集約的であり、検出ユーティリティをホストするノードのパフォーマンスに悪影響を及ぼしう。加えて、インラインIPSは、多くの誤検知攻撃診断を発生しう。さらに、インラインIPSは、インラインIPSをホストするローカルサーバにおけるトラフィックは監視しないため、偵察攻撃ユーティリティによって行われるものなどのネットワークの系統的なブローピングを検出することができない。

【0012】ネットワークベース、ホストベース、およびインラインベースのIPS技術それぞれは、上述したそれぞれの利点を有する。理想的には、不正侵入防御システムは、上記不正侵入検出戦略をすべて組み込む。加えて、IPSは、識別可能なイベントを1つまたは複数の管理設備に報告する1つまたは複数のイベント発生メカニズムを含む。イベントは、識別可能な一連のシステムまたはネットワーク状況を含んでも、また単一の識別された状況を含んでもよい。IPSはまた、解析メカニズムまたはモジュールも含み、1つまたは複数のイベント発生メカニズムにより生成されたイベントを解析することができる。不正侵入関連イベントに関連するデータを格納する格納モジュールをIPS内に備えることができる。検出された攻撃の阻止または無効化を意図するアクションを実行する対策メカニズムもIPS内に備えることができる。

【0013】セキュリティシステムの実施において無視されてきた特定の領域は、モバイルコンピュータの領域である。セルラ通信システムは概して固有のものであり、固有のアーキテクチャが過去に毀損され攻略されてきた。さらに、MicrosoftのWindows CE（登録商標）およびPalm ComputingのPalm OS（登録商標）等、いくつかのモバイル機器のオペレーティングシステムのドキュメントは公開されている。したがって、トロイの木馬型アプリケーションをこれらプラットフォームに書き込むことは簡単なことである。多くの既存のアプリケーションが、脆弱性を含むMicrosoftのWindows CE（登録商標）に移植されてきた。

【0014】

【発明が解決しようとする課題】トロイの木馬アプリケーションがモバイル機器に一旦インストールされると、機器中のデータの複製または破壊、モバイル機器を使用

しての他のシステムに対する攻撃の開始、または他の悪意を持った形態での機器の使用は簡単なことである。モバイルコンピュータ機器のコンピュータ能力が増大し、市販の無線機器の帯域が拡大し続ける場合、モバイル機器を標的とし、かつまたはモバイル機器を含むネットワークベースの攻撃がより一般的になる可能性が高い。

【0015】

【課題を解決するための手段】本発明の実施形態によれば、モバイル通信ネットワークにおいて動作可能なモバイル機器であって、中央演算処理装置による検索および実行のためにマシン読み取り可能フォーマットでデータを格納するメモリモジュールと、メモリモジュールに格納される不正侵入検出アプリケーションを実行するように動作可能なオペレーティングシステムと、を備えるモバイル機器が提供される。

【0016】本発明の別の実施形態によれば、不正侵入検出システムを管理するネットワークのノードであって、中央演算処理装置と、中央演算処理装置による検索および実行のためにマシン読み取り可能フォーマットでデータを格納するメモリモジュールと、プロトコルドライバおよび媒体アクセス制御ドライバを備えるネットワークスタックを備え、不正侵入保護システム管理アプリケーションを実行するように動作可能なオペレーティングシステムと、を備え、前記管理アプリケーションは、ネットワーク攻略ルールを定義するテキストファイル入力を受信し、テキストファイル入力、攻略シグネチャを表すマシン読み取り可能ロジックを含むシグネチャファイルに変換するように動作可能であり、ノードは、無線周波数リンクを介して前記シグネチャファイルをモバイル機器に伝送するように動作可能であるノードが提供される。

【0017】本発明、本発明の目的および利点のより完全な理解のために、次に添付図面と併せて行われる以下の説明を参照する。

【0018】

【発明の実施の形態】本発明の好ましい実施形態および本発明の利点は、同様の符号は各種図面の同様の対応する部分に使用される図面の図1ないし図6を参照することによって最もよく理解される。

【0019】図1に、コンピュータシステム毀損を実行する例示的な構成を示す。図示の例は、典型的とするマシン30に向けられた分散システム攻撃に典型的な、簡略化された分散不正侵入ネットワーク40構成を示す。攻撃マシン10は、IRC（ロボット）アプリケーションによる遠隔制御等多くの技術のうちの1つによる任意の数の攻撃エージェント20Aないし20Nによる分散攻撃の実行を指示することができる。「ゾンビ」および「攻撃エージェント」とも称される攻撃エージェント20Aないし20Nは概して、公開使用に利用可能である、または攻撃マシン10のコマンドにより分散攻撃を

起動することができるように毀損されているコンピュータである。多くの種類の分散攻撃を標的マシン30に対して開始することができる。標的マシン30は、攻撃エージェント20Aないし20Nによる同時攻撃からの広範囲のダメージを受けることがあり、攻撃エージェント20Aないし20Nはクライアント攻撃アプリケーションからも同様にダメージを受ける。分散不正侵入ネットワークは、攻撃マシン10と攻撃エージェント20Aないし20Nの間にある攻撃に関与するさらなるマシンの層を含んでもよい。これら中間マシンは一般に「ハンドラ」と呼ばれ、各ハンドラは、1つまたは複数の攻撃エージェント20Aないし20Nを制御することができる。コンピュータシステム毀損の実行について図示する構成は、例示のみを目的とするものであり、たとえば、悪意のあるブローパケットまたは標的とするマシン30の毀損を意図する他のデータを送信することにより、標的マシン30を攻撃する単一の攻撃マシン10という単純な多数の構成を毀損してもよい。標的マシンは、より大きなネットワークに接続することができ、またそうすることが多く、攻撃マシン10による標的マシンへのアクセスにより、ネットワーク内に通常あるコンピュータシステムの大きな集まりにダメージをもたらす。

【0020】図2には、本発明の実施形態によるネットワークベースと、ホストベース/ノードベース混成の不正侵入検出技術を採用した総合的な不正侵入防御システムを示す。1つまたは複数のネットワーク100は、ルータ45または他のデバイス/ノードを介してインターネット50とインタフェースすることができる。図示の例では、2つのイーサネット(登録商標)ネットワーク55および56がネットワーク100に含まれる。イーサネット(登録商標)ネットワーク55は、ウェブコンテンツサーバ270Aおよびファイル転送プロトコルコンテンツサーバ270Bを含む。イーサネット(登録商標)ネットワーク56は、ドメイン名サーバ270C、メールサーバ270D、データベースサーバ270E、およびファイナルサーバ270Fを含む。イーサネット(登録商標)55と56の中間に配置されるファイアウォール/プロキシルータ60は、セキュリティおよびアドレス解決をネットワーク56の各種システムに提供する。ネットワークのIP S機器80および81はそれぞれ、ファイアウォール/プロキシルータ60の両側で実施され、イーサネット(登録商標)55および56の1つまたは複数のエレメントに対して試みられる攻撃の監視を促進し、またファイアウォール/プロキシルータ60の侵入に成功した成功攻撃の記録を促進する。ネットワークベースのIP S機器80および81はそれぞれ、取り込んだネットワークフレームを比較することのできる既知の攻撃シグネチャまたはルールのデータベース80Aおよび81Aをそれぞれ備える(か、あるいは、接続される)。あるいは、単一データベース(図示せず)をネットワ

ク100内の中央に配置し、ネットワークベースのIP S機器80および81がこれにアクセスしてもよい。したがって、ネットワークベースのIP S機器80は、イーサネット50からネットワーク100へのインバウンドでイーサネット(登録商標)ネットワーク55に到来するすべてのパケットを監視することができる。同様に、ネットワークベースのIP S機器81は、イーサネット(登録商標)ネットワーク56への送出について、ファイアウォール/プロキシルータ60によって渡されるすべてのパケットを監視し比較することができる。IP S管理ノード85もまたネットワーク100の一部であることができ、ネットワーク100におけるIP Sコンポーネントの構成および管理を促進する。

【0021】上記ネットワークベースの不正侵入防御システムの欠点を鑑みて、ホストベースとノードベース混成の不正侵入防御システムが、安全なネットワーク100におけるイーサネット(登録商標)ネットワーク55および56の、サーバ270Aないし270N(本明細書では「ノード」とも称される)等各各種ノードそれぞれに実施することが好ましい。管理ノード85は、ネットワークベースのIP S機器80および81のいずれか1つ、ならびに実施されるエージェントベースとノードベース混成のIP Sを有する、ネットワーク100のノードのいずれかにより不正侵入イベントが検出されると、ネットワーク100内の各ノードから警告を受信する。加えて、各ノード270Aないし270Fはそれぞれ、不正侵入関連イベントを保存し、不正侵入関連報告を生成し、ローカルネットワークフレームおよび/またはパケットを検査するためのシグネチャファイルを格納するローカルファイルシステムを採用する。

【0022】好ましくは、ネットワークベースのIP S機器80および81は、ネットワーク100の関連イーサネット(登録商標)55および56上のネットワークトラヒックの監視専用のエンティティである。高速ネットワークでの不正侵入検出を促進するために、ネットワークベースのIP S機器80および81は、好ましくは、各イーサネット(登録商標)ネットワーク55および56に到来するときにパケットを取り込むために容量の大きなキャプチャRAMを備える。加えて、ネットワークベースのIP S機器80および81はそれぞれ、ネットワークトラヒックをフィルタリングするためにハードウェアベースのフィルタを備えることが好ましいが、ネットワークベースのIP S機器80および81によるIP Sフィルタリングはソフトウェアで実施してもよい。さらに、ネットワークベースのIP S機器80および81は、例えば、IP S管理ノード85の要求により、共通ネットワーク上のすべての機器ではなく1つまたは複数の特定の機器を監視するように構成してもよい。たとえば、ウェブサーバ270Aにアドレス指定されたネットワークデータトラヒックのみを監視するようにネットワ

ークベースのIPS機器80に指示してもよい。

【0023】ホストベース/ノードベース混成の不正侵入防御システム技術は、ネットワーク攻撃の標的となるイーサネット(登録商標)ネットワーク5および56上のすべてのノード270Aないし270Nに実施することができる。概して、各ノードは、中央演算処理装置(CPU)と、CPUにより検索および実行されるマシン読み取り可能コードを格納するように動作可能なメモリモジュールと、を備える再プログラム可能なコンピュータを備えると共に、接続されるディスプレイモニタ、キーボード、マウス、または別の機器等各種周辺機器をさらに備えることができる。磁気ディスク、光ディスク、またはデータを格納するように動作可能な別のコンピュータ等格納媒体は、メモリモジュールに接続し、メモリモジュールによりアクセス可能であり、ローカル不正侵入イベントおよび不正侵入イベント報告を保存する1つまたは複数のデータベースを提供することもできる。たとえば、各ノードのブートアップ時にオペレーティングシステムをメモリモジュールにロードすることができ、オペレーティングシステムは、プロトコルスタックのインスタンスならびに周辺ハードウェアとのインタフェース、タスクのスケジューリング、記憶割り当て、ならびに他のシステムタスク等タスクに必要な各種低レベルソフトウェアモジュールを含む。したがって、本発明のホストベースとノードベース混成のIPSによって保護される各ノードは、磁気ハードディスク中などノード内に維持され、オペレーティングシステムによって検索可能であり、中央演算処理装置によって実行可能なIPSソフトウェアアプリケーションを有する。加えて、IPSアプリケーションのインスタンスを実行する各ノードは、ドキュメント化された攻撃のシグネチャ記述を格納構成からフェッチし、データのバケットまたはフレームと比較してその間の対応を検出するローカルデータベースを有する。IDSサーバにおけるバケットまたはフレーム間で対応が検出されると、各種セキュリティ手順の任意の1つまたは複数を実行することができる。

【0024】図2を参照して述べるIPSは、任意の数のプラットフォームで実施することができる。本明細書に述べるホストベース/ノードベース混成のIPSアプリケーションの各インスタンスは、好ましくは、主記憶構成に格納され、中央演算処理装置上で実行され、ホストノードを標的とする攻撃を検出しようとするWindows NT(登録商標)4.0等オペレーティングシステムの制御下で動作するウェブサーバ270A等、ネットワークノード上で実施される。図2に示す特定のネットワーク10は、例示を目的とし、任意の数のネットワークサーバを含む。たとえば、企業および他の大規模ネットワークは通常、同様のサービスを提供する個々のシステムを多く含む。たとえば、企業ネットワークは、数百

の個々のウェブサーバ、メールサーバ、FTPサーバ、および共通のデータサービスを提供する他のシステムを含む。

【0025】IPSアプリケーションのインスタンスを組み込んだノードの各オペレーティングシステムは、図3に示すように、ネットワーク、たとえばインターネットまたはイントラネットから標的ノードが受信するフレームのエントリポイントを定義するネットワークプロトコルスタック90をさらに含む。図示のネットワークスタック90は、既知のWindows NT(登録商標)システムネットワークプロトコルスタックを表し、本発明の考察および理解を容易にするために選択されたものである。しかし、本発明は、図示のネットワークスタック90の特定の実施に限定されず、スタック90は本発明の理解を容易にするために述べられることを理解されたい。ネットワークスタック90は、転送ドライバインタフェース(TDI)125、転送ドライバ130、プロトコルドライバ135、および物理的な媒体101とインタフェースする媒体アクセス制御(MAC)ドライバ145を含む。転送ドライバインタフェース125は、転送ドライバ130とより上位のファイルシステムドライバとをインタフェースするように機能する。したがって、TDI125は、ネットワークリダイレクタ(redirector)等オペレーティングシステムドライバが適切なプロトコルドライバ135とのセッションを起動する、またはバインディングできるようにする。したがって、リダイレクタは、適切なプロトコル、たとえばUDP、TCP、NetBEUI、または他のネットワーク、またはトランスポートレイヤプロトコル、にアクセスすることができ、これによりリダイレクタがプロトコルから独立したものになる。プロトコルドライバ135は、物理的な媒体101を介してネットワークプロトコルスタック90をホストするコンピュータからネットワーク上の別のコンピュータまたは機器もしくは別のネットワークに送信されるデータバケットを作成する。NTネットワークプロトコルスタックによりサポートされる典型的なプロトコルは、NetBEUI、TCP/IP、NWLink、データリンク制御(DLC)、およびAppleTalkを含むが、別の転送および/またはネットワークプロトコルも含みうる。MACドライバ145、たとえばイーサネット(登録商標)ドライバ、トークンリングドライバ、または他のネットワークングドライバは、適切なフォーマットおよび同軸ケーブルまたは別の伝送媒体等物理的な媒体101とのインタフェースを提供する。

【0026】ホストベースのIPSの能力は、ファイルシステムイベント、レジストリアクセス、成功したセキュリティイベント、失敗したセキュリティイベント、および疑いのあるプロセスのアプリケーション監視を含み、Microsoft IISおよびSQLサーバ等

ネットワークアクセスアプリケーションは、関連するプロセスも監視することができる。

【0027】本発明の実施形態によるインライン、ノードベースの監視技術の実施により、特定のIPSホストにおける不正侵入を防御することができる。インラインIPSは、好ましくは、ホストベース/ノードベース混成のIPSの一部として含まれるが、任意のホストベースのIPSシステムから独立して実施してもよい。インラインIPSは、ホストノードで受信するパケットを解析し、ネットワークレイファイリングにより既知のシグネチャのデータベースに対してシグネチャ解析を実行する。

【0028】図4には、IPSアプリケーション91のインスタンスを実行し、したがってIPSサーバとして動作しうるネットワークノード270を示す。IPSアプリケーション91は、本出願の対応米国出願と同時出願された「Method, Computer Readable Medium, and Node for a Three-Layered Intrusion Prevention System for Detecting Network Exploits」と題する同時係属中の米国出願に記載の三層IPSとして実施してもよく、またサーバアプリケーションおよび/またはクライアントアプリケーションを含んでもよい。ネットワークノード270は概して、中央演算処理装置(CPU)272と、バス(図示せず)を介してCPU272により検索可能であり実行可能なマシン読み取り可能コードを格納するように動作可能なメモリモジュール274と、を備える。磁気ディスク、光ディスク、またはデータを格納するように動作可能な別のコンポーネント等格納媒体276は、メモリモジュール274に接続することができ、同様にバスによりアクセス可能である。たとえば、ノード270のブートアップ時にオペレーティングシステム275をメモリモジュール274にロードすることができ、オペレーティングシステム275は、プロトコルスタック90のインスタンスを含むことができ、また格納媒体276からロードされる不正侵入防御システムアプリケーション91を有する。本出願の対応米国出願と同時出願された「Method, Node and Computer Readable Medium for Identifying Data in a Network Exploit」と題する同時継続中の米国出願に記載の例示的な形態の1つまたは複数のネットワーク攻撃ルールをマシン読み取り可能シグネチャにコンパイルし、メモリモジュール274にロード可能なデータベース277内に格納され、ネットワークフレームおよび/またはパケットの解析を促進するために、IPSアプリケーション91のモジュール、たとえばIPSアプリケーション91のインライン不正侵入検出モジュールの結合プロセスエンジンによって検索することができる。結合プロセスエンジンを含むインライン不正侵入検出アプリケーションおよびIPSアプリケーション91に組み込むことのできる入出力制御レイヤの例示的な構成は、本出願の対応

米国出願と同時出願された「Method, Node and Computer Readable Medium for Inline Intrusion Detection on a Network Stack」と題する同時継続中の米国出願に記載されている。

【0029】図5には、ネットワーク100のIPSの管理ノード85として動作しうる例示的なネットワークノードを示す。管理ノード85は概して、CPU272と、バス(図示せず)を介してCPU272により検索可能であり実行可能なマシン読み取り可能コードを格納するように動作可能なメモリモジュール274と、を備える。磁気ディスク、光ディスク、またはデータを格納するように動作可能な別のコンポーネント等格納媒体276は、メモリモジュール274に接続することができ、同様にバスによりアクセス可能である。たとえば、ノード85のブートアップ時にオペレーティングシステム275をメモリモジュール274にロードすることができ、オペレーティングシステム275は、プロトコルスタック90のインスタンスを含む。オペレーティングシステム275は、IPS管理アプリケーション279を格納媒体276からフェッチし、管理アプリケーション279を、CPU272による実行可能なメモリモジュール274にロードするように動作可能である。ノード85は、好ましくは、接続されたキーボード等入力装置281と、モニタ等出力装置282とを有する。

【0030】管理ノード85の操作者は、入力装置281を介して1つまたは複数のテキストファイル277Aないし277Nを入力することができる。各テキストファイル277Aないし277Nは、ネットワークベースの攻撃を定義し、IPSアプリケーション91が識別されたパケットおよび/またはフレームをデータベースに記録させる命令、識別されたパケットおよび/またはフレームをドロップする命令、および/またはIPSが記述された攻撃シグネチャと関連する不正侵入関連イベントを評価したとき他のセキュリティ対策を実行する指示等、攻撃シグネチャならびにIPS指示の論理的な記述を含む。各テキストファイル277Aないし277Nは、格納媒体276上のデータベース278Aに格納し、コンパイル280により、データベース278Bに格納される各マシン読み取り可能シグネチャファイル281Aないし281Nにコンパイルすることができる。各マシン読み取り可能シグネチャファイル281Aないし281Nは、関連する各テキストファイル277Aないし277Nに記述される攻撃シグネチャを表す値論理を含み、各テキストファイルに含まれる1つまたは複数の指示を表す論理を含むことができる。管理ノード85の操作者は、入力装置281を介してIPSアプリケーション279のクライアントアプリケーションとの対話を通して、データベース278Bに格納されている1つまたは複数のマシン読み取り可能シグネチャファイル(本明細書では概して「シグネチャファイル」とも称

される)をネットワーク100中の1つまたは複数のノードに伝送するように、管理ノード85に周期的に指示しうる。あるいは、シグネチャファイル281Aないし281Nは、コンパクトディスク、磁気フレキシブルディスク、または別のポータブル格納媒体等コンピュータ読み取り可能媒体に格納し、ネットワーク100中のノード270にインストールしてもよい。アプリケーション279は、好ましくは、このようなシグネチャファイル281Aないし281Nすべてまたはその1つまたは複数のサブセットをネットワーク100中の1つまたは複数のノードに伝送するように動作可能である。好ましくは、IP Sアプリケーション279は、ノード85の操作者によるコマンドの入力を促進するために、出力装置282上でグラフィカルユーザインタフェースを提供する。

【0031】図6には、本発明のモバイル機器にサービス提供しうるモバイル通信システム(MTS)300を示す。例示的なモバイル通信システム300について、GSM(Global System for Mobile communications)規格の一般的なインフラストラクチャおよび名称に従って説明するが、本発明はかかるシステムでの用途に限定されず、説明は例示のみを目的とする。MTS300は概して、1つまたは複数の交換システム(SS)305ないし306と、モバイル通信サービスを1つまたは複数のモバイル機器355に提供する基地局サブシステム(BSS)340ないし341を含む。モバイル機器355は、モバイル端末として機能しうる、無線モデムを備えたモバイルラップトップコンピュータ、無線個人情報端末、ページャ、データ可能セルラ電話、または他の無線通信装置等各種形態をとることができる。モバイル機器355は、各BSS340ないし341内に含まれる1つまたは複数の送受基地局(BTS)352Aないし352Cおよび353Aないし353Cと直接通信する。各BSS、たとえばBSS340は通常、1つまたは複数の地理的に多様なBTS、たとえばBTS352Aないし352Cを含む。1つのBTSグループ、たとえばBTSグループ352ないし353の1つは、各BSS340ないし341内に含まれ、無線ネットワークコントローラとも呼ばれる基地局コントローラ(BSC)345ないし346によって管理される。各BSS340ないし341は、交換システム305ないし306内に含まれる各モバイルサービス交換センタ(MSC)310ないし311と通信し、これによって制御される。個々のBTS352Aないし352Cおよび353Aないし353Cはそれぞれ、無線チャネルセットに対して動作する無線線を画定し、それによって1つまたは複数のモバイル機器355にサービスを提供する。したがって、各BSC345ないし346は、これによって制御される複数のBTS352Aないし352Cおよび353Aないし353Cそれぞれに対応する複数の

セルを有する。

【0032】交換システム305ないし306はそれぞれ、各種ハードウェアおよびソフトウェアで実施される複数の機能ユニットを含む。概して、各SS305ないし306はそれぞれ、MSC310ないし311、ビクターロケーションレジスタ(VLR)375ないし376、ホームロケーションレジスタ(HLR)370ないし371、認証センタ381ないし382、および機器識別レジスタ385ないし386を含む。MTS300内で動作可能なモバイル機器355は、ホームレジスタと指定されるレジスタを有する。本例では、また以下に提供する例では、HLR371がモバイル機器355のホームレジスタを表す。HLR371は、ホームレジスタと指定されたHLR371を有するモバイル機器のプロファイルを含むデータベースである。HLR371におけるモバイル機器355のプロファイル内に含まれる情報は、各種加入者情報、たとえば国際移動局機器識別(IMEI)、電子シリアルナンバー(ESN)、および認証能力パラメータ等認証パラメータ、ならびに加入に含まれるサービスを定義するアクセスポイント名(APN)等加入サービスパラメータを含む。加えて、モバイル機器355のHLR371プロファイルは、MTS300内の現在、または最後にわかつてのモバイルデバイス355のロケーションに関連するデータ、たとえばロケーションエリア識別子を含む。モバイル機器355に関連するHLR371内に含まれるロケーションデータは、動的性質のものである。すなわち、モバイル機器355がMTS300を通して移動するにつれて変化する。各MSC310ないし311は、2つ以上のBSC345ないし346を制御することができ、通常はそうすることを理解されたい。図6では、本発明の説明を簡明にするために、1つのみの各BSC345ないし346がMSC310ないし311によって制御されて示される。

【0033】VLR375ないし376は、関連するMSC310ないし311によって現在サービス提供されているすべてのモバイル機器355についての情報を含むデータベースである。たとえば、VLR376は、MSC311によってサービス提供されている各モバイル機器に関連する情報を含み、したがって関連するBSC346によって制御されるBTS353Aないし353Cによって現在サービス提供されているすべてのモバイル機器に関連する情報を含む。モバイル機器355が、別のMSCにより制御されるBTSのセルカバレッジエリアに入る、たとえばモバイル機器355が、BTS352Cによって提供されるカバレッジエリアにローミングすると、BTS352Cは関連するSS305のVLR375が、モバイル機器355に関連する加入者情報について、モバイル機器355のHLR371に問い合わせる。次いで、この情報がVLR375に転送され

る。同時に、VLR375が、モバイル機器355の新しい位置を示すロケーション情報をHLR371に伝送する。次いで、モバイル機器355に関連するHLRプロファイルが、モバイル機器355の位置を適宜示すように更新される。このロケーション情報は概して、ロケーションエリア識別子に限られる。ローミング中のモバイルデバイス355に関連するVLR375に伝送される情報により概して、たとえばモバイル機器355の認証および加入サービスパラメータについて、HLR371にさらに問い合わせることなく、呼のセットアップおよびモバイル機器355の処理が可能である。このように、モバイル機器355が、呼、たとえばデータ呼を実行するか受信しようとするときに、SS305は、モバイル機器355に適宜サービスを提供するように、セットアップを実行し、サービス機能を切り換えるために必要な情報を有する。加えて、VLR375は通常、HLR371よりも正確なモバイル機器355についての情報を含み、たとえば、VLR375は、モバイル機器355にサービス提供している特定のBSCを示すBSC識別子を含みうる。

【0034】各SS305ないし306は、各SS305ないし306のHLR370ないし371に接続される認証センタ(AUC)381ないし382も備える。AUC381ないし382は、モバイル機器355に、モバイル機器355ないし356を認証するために、認証パラメータをHLR370ないし371に提供する。AUC381ないし382は、モバイル機器355との通信を安全にするために使用される暗号鍵を生成することもできる。加えて、SS305ないし306は、1つまたは複数のモバイル機器を一意に識別するために使用される国際移動局機器識別を含む機器識別レジスタ(EIR)385ないし386データベースも備える。EIR385ないし386は、MTS300におけるサービス要求するモバイル機器355を検証するために使用される。

【0035】たとえばインターネットサービスを提供するために、GPRS (General packet radio service) をMTS300に備えることができる。GPRSは、回線交換ではなくパケット交換のデータサービスである。パケットデータネットワーク360に接続して無線インターネットサービス等GPRSにアクセスするために、ゲートウェイGPRSサポートノード(GGSN)330が通常MTS300に含まれる。たとえばパケットデータプロトコル(PDP)セッションの管理、ならびにモバイル機器の認証、識別、およびIMEI問い合わせ等管理機能の実行等、1つまたは複数のサービス提供GPRSサポートノード(SGSN)320ないし321が、モバイル機器355にGPRSサービスへのアクセスを提供するために、MTS300に含まれる。したがって、GGSN330は、パケットデータネットワーク360へのモバイル通信システム300

のインタフェースを提供し、一方、SGSN320ないし321は、モバイル機器355が、モバイル通信システム300インフラストラクチャを介してGGSN330、ひいてはパケットデータネットワーク360と通信できるようにする。

【0036】GPRS可能モバイル機器は、まず接続手順を実行することによりパケットデータネットワークにアクセスしてもいい。大まかに言えば、接続手順は、モバイル機器にサービス提供しているSGSNに接続要求メッセージを送信することによって開始される。例示的な本例では、モバイル機器355が現在BSS341により提供されているセル内にある。SGSN321は、通信チャネルによりBSS341に接続され、したがってモバイル機器355にGPRSサービスを提供する責任を担う。次いで、SGSN321は、モバイル機器355を識別し認証した後に、ロケーション更新メッセージをHLR371に送信する。モバイル機器の認証は、モバイル機器のホームレジスタを有するSS306における各種モジュールのSGSN321による問い合わせを含んでもいい。たとえば、SGSNは、AUC382またはEIR386に問い合わせる。これに応答して、HLR371が加入者情報ならびにロケーション更新の承認をSGSN321に送信する。

【0037】パケット通信に携わるために、接続されたモバイル機器355は次いで、起動手順、たとえばPDP起動を実行しなければならない。概して、起動要求メッセージがモバイル機器355からSGSN321に伝送される。次いで、SGSN321がGGSN330にコンタクトをとり、PDP起動を要求する。GGSN330は、データネットワーク360からのパケットデータをモバイル機器355に適宜ルーティングすることができるよう、モバイル機器355にサービス提供しているSGSN321のアドレスの記録を維持する。次いで、GGSN330は、モバイル機器が別のSGSNによってサービス提供されるBTSにより提供されるセルにローミングするときは常に、たとえばモバイル機器355がSGSN320によってサービス提供されるBTS352Cにより提供されるセルにローミングするとき、SGSNアドレスを更新する。

【0038】本発明のモバイル機器は、ネットワーク300との通信の送受信を促進するために、ネットワークスタック90のインスタンスまたはその変形を維持することができる。本発明の無線実施では、ネットワーク媒体101は、モバイル機器355と、BTS352Aないし352Cおよび/または353Aないし353Cの1つで終端する無線周波数リンクを含む。モバイル機器355は、ネットワーク270の要素、すなわちCPU272、メモリモジュール274を組み込み、またモバイル機器355がIPアプリケーション91を実行するように動作可能のように格納媒体276

も備えることができる。上述したように、IPSアプリケーション91は、クライアントおよび/またはサーバアプリケーションを含む。クライアントアプリケーションは、好ましくは、モバイル機器355で維持され実行される。サーバアプリケーションは、モバイル機器355で実行しても、あるいは例えばSS306によりネットワーク300上で実行し、モバイル機器355との無線通信に携わってもよく、IPSアプリケーション91のクライアントアプリケーションの動作を促進する。たとえば、モバイル機器355において不正侵入関連イベントを検出するように、IPSアプリケーション91が利用するマシン読み取り可能シグネチャファイルはモバイル機器355に提供する。管理ノード85の機能性は、SS305および306内の管理アプリケーション279を実行するCPUを含むことにより交換システムに組み込むことができる。したがって、モバイル機器355に向けられるネットワーク攻撃を検出し阻止することができる。

【0039】本発明の態様を以下に例示する。

【0040】1. モバイル通信ネットワーク(300)において動作可能なモバイル機器(355)であって、中央演算処理装置(272)による検索および実行のためにマシン読み取り可能フォーマットでデータを格納するメモリモジュール(274)と、該メモリモジュール(274)に格納される不正侵入検出アプリケーション(91)を実行するように動作可能なオペレーティングシステム(275)と、を備えるモバイル機器。

【0041】2. 前記オペレーティングシステム(275)は、プロトコルドライバ(135)と、媒体アクセス制御ドライバ(145)と、を備えるネットワークスタック(90)をさらに備え、前記不正侵入検出アプリケーション(91)は、前記プロトコルドライバ(135)と前記媒体アクセス制御ドライバ(145)とに結び付けられた中間ドライバを備える、上記1記載のモバイル機器。

【0042】3. 前記不正侵入検出アプリケーション(91)は、結合プロセスエンジンと、入出力制御レイヤと、をさらに備え、前記入出力制御レイヤは、シグネチャファイル(281Aないし281N)を受信し、該シグネチャファイル(281Aないし281N)を前記結合プロセスエンジンに渡すように動作可能であり、前記結合プロセスエンジンは、前記シグネチャファイル(281Aないし281N)を使用してデータバケットを解析するように動作可能である、上記1または2記載のモバイル機器。

【0043】4. 格納媒体(276)をさらに備え、該格納媒体(276)は、複数のシグネチャファイル(281Aないし281N)のデータベース(277)を維持するように動作可能である、上記1ないし3のいずれか一項記載のモバイル機器。

【0044】5. 前記不正侵入検出アプリケーション(91)は、前記シグネチャファイル(281Aないし281N)とデータバケットの間の対応を識別し、該対応が識別されると、前記データバケットが不正侵入に関連するものであるという判断が行われる、上記3または4記載のモバイル機器。

【0045】6. 前記シグネチャファイル(281Aないし281N)は、前記データバケットが不正侵入に関連するものであると決定されると、前記プロセッサ(272)が実行すべきプロセスを定義する指示を含む、上記3ないし5のいずれか一項記載のモバイル機器。

【0046】7. 前記不正侵入検出アプリケーション(91)は、前記モバイル機器(355)の不正侵入に関連するイベントを識別するように動作可能であり、前記モバイル機器(355)は、不正侵入に関連するイベントデータを前記ネットワーク(300)の管理ノード(85)に提供するように動作可能である、上記1ないし6のいずれか一項記載のモバイル機器。

【0047】8. 前記管理ノード(85)は、モバイル通信ネットワーク交換システム(305ないし306)である、上記7記載のモバイル機器。

【0048】9. 不正侵入検出システムを管理するネットワーク(300)のノード(85)であって、中央演算処理装置(272)による検索および実行のためにマシン読み取り可能フォーマットでデータを格納するメモリモジュール(274)と、プロトコルドライバ(135)および媒体アクセス制御ドライバ(145)を備えるネットワークスタック(90)を備え、不正侵入保護システム管理アプリケーション(279)を実行するように動作可能なオペレーティングシステム(275)と、を備え、前記管理アプリケーション(279)は、ネットワーク攻撃ルールを定義するテキストファイル入力(277Aないし277N)を受信し、前記テキストファイル入力(277Aないし277N)を、攻撃シグネチャを表すマシン読み取り可能ロジックを含むシグネチャファイル(281Aないし281N)に変換するように動作可能であり、前記ノード(85)は、無線周波数リンクを介して前記シグネチャファイル(281Aないし281N)をモバイル機器(355)に伝送するように動作可能である、ノード。

【0049】10. 前記無線周波数リンクは、モバイル機器(355)およびモバイル通信ネットワーク(300)の送受信基地局(352Aないし352C、353Aないし353C)で終端する、上記9記載のノード。

【図面の簡単な説明】

【図1】従来技術によるコンピュータシステム毀損を実行する例示的な構成を示す。

【図2】本発明の実施形態によるネットワークベースと、ホストベースおよびノードベース混成の不正侵入検出技術を採用した総合的な不正侵入防御システムを示す。

す。

【図3】従来技術による例示的なネットワークプロトコルスタックである。

【図4】本発明の実施形態による不正侵入保護システムアプリケーションのインスタンスを実行しうるネットワークノードを示す。

【図5】本発明の実施形態による不正侵入保護システムによって保護されるネットワーク内の管理ノードとして*

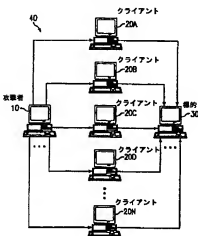
*動作しうる例示的なネットワークノードを示す。

【図6】本発明の実施形態によるモバイル機器にサービスを提供しうるモバイル通信システムの模式図である。

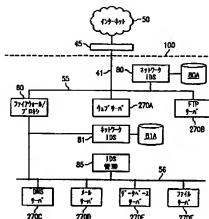
【符号の説明】

- 90 ネットワークスタック
91 不正侵入検出アプリケーション
275 オペレーティングシステム

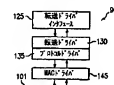
【図1】



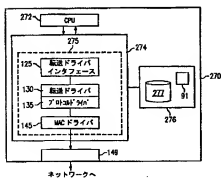
【図2】



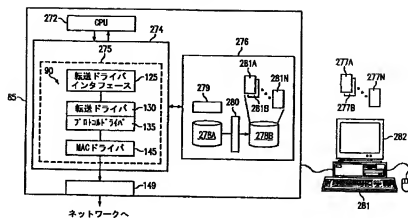
【図3】



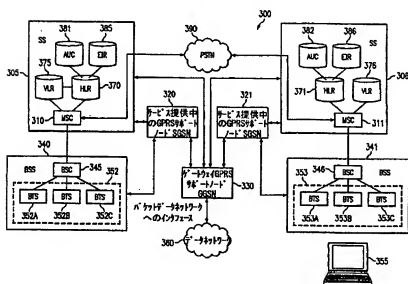
【図4】



【図5】



【図6】



フロントページの続き

(72)発明者 リチャード・ルイス・シェルト
アメリカ合衆国27607ノース・カロライナ
州ローリー、プリンウッド・コート 117

(72)発明者 ジョージ・サイモン・ゲイルズ
アメリカ合衆国75025テキサス州プラノ、
クリア・フィールド・ドライブ 2456
Fターム(参考) 5B085 A408 BEO4 BC01 BC02 BC07

【公報種別】特許法第17条の2の規定による補正の掲載

【部門区分】第6部門第3区分

【発行日】平成17年12月2日(2005.12.2)

【公開番号】特開2003-228552(P2003-228552A)

【公開日】平成15年8月15日(2003.8.15)

【出願番号】特願2002-304068(P2002-304068)

【国際特許分類第7版】

G 0 6 F 15/00

【F1】

G 0 6 F 15/00 3 3 0 A

【手続補正書】

【提出日】平成17年10月18日(2005.10.18)

【手続補正1】

【補正対象書類名】明細書

【補正対象項目名】特許請求の範囲

【補正方法】変更

【補正の内容】

【特許請求の範囲】

【請求項1】 モバイル通信ネットワークにおいて動作可能なモバイル機器であって

、中央演算処理装置による検索および実行のためにマシン読み取り可能フォーマットでデータを格納するメモリモジュールと、

該メモリモジュールに格納される不正侵入検出アプリケーションを実行するように動作可能なオペレーティングシステムと、を備えるモバイル機器。

【請求項2】 前記オペレーティングシステムは、プロトコルドライバと、媒体アクセス制御ドライバと、を備えるネットワークスタックをさらに備え、前記不正侵入検出アプリケーションは、前記プロトコルドライバと前記媒体アクセス制御ドライバとに結び付けられた中間ドライバを備え、請求項1記載のモバイル機器。

【請求項3】 前記不正侵入検出アプリケーションは、結合プロセスエンジンと、入出力制御レイヤと、をさらに備え、前記入出力制御レイヤは、シグネチャファイルを受信し、該シグネチャファイルを前記結合プロセスエンジンに渡すように動作可能であり、前記結合プロセスエンジンは、前記シグネチャファイルを使用してデータパケットを解析するように動作可能である、請求項1または2記載のモバイル機器。

【請求項4】 該格納媒体をさらに備え、該格納媒体は、複数のシグネチャファイルのデータベースを維持するように動作可能である、請求項1ないし3のいずれか一項記載のモバイル機器。

【請求項5】 前記不正侵入検出アプリケーションは、前記シグネチャファイルとデータパケットの間の対応を識別し、該対応が識別されると、前記データパケットが不正侵入に関連するものであるという判断が行われる、請求項3または4記載のモバイル機器。

【請求項6】 前記シグネチャファイルは、前記データパケットが不正侵入に関連するものであると決定されると、前記プロセッサが実行すべきプロセスを定義する指示を含む、請求項3ないし5のいずれか一項記載のモバイル機器。

【請求項7】 前記不正侵入検出アプリケーションは、前記モバイル機器の不正侵入に関連するイベントを識別するように動作可能であり、前記モバイル機器は、不正侵入に関連するイベントデータを前記ネットワークの管理ノードに提供するように動作可能である、請求項1ないし6のいずれか一項記載のモバイル機器。

【請求項8】 前記管理ノードは、モバイル通信ネットワーク交換システムである、請求項7記載のモバイル機器。

【請求項 9】 不正侵入検出システムを管理するネットワークのノードであって、中央演算処理装置による検索および実行のためにマシン読み取り可能フォーマットでデータを格納するメモリモジュールと、

プロトコルドライバおよび媒体アクセス制御ドライバを備えるネットワークスタックを備え、不正侵入保護システム管理アプリケーションを実行するように動作可能なオペレーティングシステムと、を備え、前記管理アプリケーションは、ネットワーク攻略ルールを定義するテキストファイル入力を受信し、前記テキストファイル入力を、攻略シグネチャを表すマシン読み取り可能ロジックを含むシグネチャファイルに変換するように動作可能であり、前記ノードは、無線周波数リンクを介して前記シグネチャファイルをモバイル機器に伝送するように動作可能である、ノード。

【請求項 10】 前記無線周波数リンクは、モバイル機器およびモバイル通信ネットワークの送受信基地局で終端する、請求項 9 記載のノード。